IN THE CLAIMS

Please amend the claims as follows:

1. (Currently Amended) A method of controlling content usage in a wireless communication device having two or more processors using a decryption key that is divided into at least first, second and third key-shares, the method comprising:

pre-storing the third key-share in the wireless communication device;

providing the wireless communication device the first key-share in response to a request for content; and

providing the wireless communication device the second key-share when credit of a user of the wireless communication device is verified,

wherein upon receipt of the content, ~~by~~ a security processor of the wireless communication device combines the first and second key-shares with the third key-share for use in decrypting the content,

wherein the security processor further monitors usage of the content and purges at least one of the key shares when usage of the content exceeds one or more measurement parameters,

wherein the security processor further authenticates the measurement parameters using an authentication code to help prevent tampering with the measurement parameters,

wherein the decrypted content is provided to a communication processor of the wireless communication device for playing, ~~and~~

wherein the measurement parameters are secured by the authentication code and provided by a security server over a wireless link along with encrypted content,

wherein the two or more processors include the security processor and the communication processor located within a processor area of an integrated circuit, and

wherein communications between the security processor and the communication processor take place within the processor area to inhibit unauthorized interception of the decrypted content and unauthorized interception of the third key-share stored therein.

2. (Currently Amended) The method as claimed in claim [[15]] 1 wherein:

the security processor purges at least one of the key shares when usage of the content exceeds a service limit indicated by the measurement parameters or when the authentication code fails to authenticate.

3. (Currently Amended) The method as claimed in claim 2 further comprising:

receiving the request for the content from the wireless communication device, the request identifying the content and the measurement parameters for the content; and

encrypting the content in the security server with an encryption key corresponding to the decryption key,

wherein the third key-share is pre-stored in the processor area of the wireless communication device prior to encrypting the content.

4. (Currently Amended) The method as claimed in claim [[15]] 1 further comprising:

in response to verification of the user's credit, receiving the content from a content server at the security server;

encrypting the content in the security server with an encryption key corresponding to the decryption key; and

providing the encrypted content from the security server to the wireless communication device over the wireless link.

5. (Previously Presented) The method as claimed in claim 4 wherein the content server and the security server communicate over a non-secure network, and

wherein the method includes the content server adding security to the content prior to providing the content to the security server.

6. (Previously Presented) The method as claimed in claim 4 wherein the providing the first of the key-shares is performed by the security server over the wireless link in response to either the receipt of content at the security server or the encryption of the content by the security server in communication with the wireless communication device.

7. (Currently Amended) The method as claimed in claim 1 wherein ~~the third~~ a fourth key-share is pre-stored in a subscriber identity module (SIM) associated with the user,

wherein ~~a fourth of~~ the third key-share[[s]] is pre-stored in the processor area of the wireless communication device and associated with the security processor of the wireless communication device, and

wherein the security processor combines the first, second, third and fourth key-shares to generate the decryption key and decrypt the encrypted content.

8. (Previously Presented) The method as claimed in claim 1 wherein the verifying credit of the user and the providing the second of the key-shares to the wireless communication device are performed by a finance server in communication with the wireless communication device.

9. (Currently Amended) The method as claimed in claim 1 further comprising generating the key-shares from the decryption key using a key-splitting technique, and

wherein the security processor and the communication processor are fabricated within an application specific integrated circuit (ASIC).

10. (Previously Presented) The method as claimed in claim 2 wherein the content comprises at least one of either video content or music content.

11. (Previously Presented) The method as claimed in claim 2 further comprising generating the set of measuring parameters comprising at least one of a date-limit, a run-time limit, and an iteration limit, and

wherein the wireless communication device monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares when the usage exceeds one of the measurement parameters of the set.

12. (Previously Presented) The method as claimed in claim 11 further comprising a content server defining the set of measurement parameters based on preferences of a content provider.

13. (Previously Presented) The method as claimed in claim 11 wherein the date-limit defines an end calendar date for playing the content,

wherein the run-time limit defines a maximum amount of time for playing portions of the content, and

wherein the iteration limit defines a maximum number of times for playing the content or portions thereof.

14. (Cancelled)

15. (Currently Amended) The method as claimed in claim 1 wherein the wireless communication device receives the first and second of the key-shares over the wireless link, and

wherein the third key-share is pre-stored in the processor area of the wireless communication device prior to the user generating the request for the content and prior to a security server sending the content and the second key-share to the wireless communication device.

16. (Currently Amended) A multiprocessor processing system for a wireless communication device, the processing system comprising:

a security processor to combine first, second and third key-shares to generate a decryption key to decrypt content for the processing system, the security processor to monitor usage of the content and to purge at least one of the key-shares when the usage exceeds a measurement parameter; and

a communications processor to play decrypted content received from the security processor,

wherein the security processor and the communication processor are located within a processor area of an integrated circuit,

wherein communications between the security processor and the communication processor take place within the processor area to inhibit unauthorized interception of the decrypted content and interception of the third key-share stored in the processor area, wherein the wireless communication device has the third key-share pre-stored in the processor area ~~therein~~ and receives the first key-share and the second key-share over a wireless link in response to a request for content and a verification of a user's credit,

wherein the security processor authenticates the measurement parameters with an authentication code to help prevent tampering with the measurement parameters, and

wherein the measurement parameters are secured by the authentication code and provided by a security server over the wireless link along with the encrypted content or when the authentication code fails to authenticate.

17. (Currently Amended) The processing system as claimed in claim 16 wherein the security processor portion purges at least one of the key-shares when ~~when~~ usage of the content exceeds a service limit indicated by the measurement parameters.

18. (Currently Amended) The processing system as claimed in claim 16 wherein the security processor ~~portion has the third key-share pre-stored therein,~~ retrieves a fourth key-share from a subscriber identity module inserted into the wireless communication device, and receives the second key-share from a finance server when a user's credit is verified for use of the content.

19. (Previously Presented) The processing system as claimed in claim 16 wherein the measurement parameters comprise at least one of a date-limit, a run-time limit, and an iteration limit.

20. (Currently Amended) The processing system as claimed in claim 16 further comprising an applications processor located with the processor area to process applications running on the wireless communication device, and

wherein the security processor, the communications processor and the applications processor are ~~part of a processor area and~~ fabricated ~~on~~ within an application specific integrated circuit (ASIC).

21. (Currently Amended) A wireless communication device comprising:

a processor area of an integrated circuit having a communications processor and a security processor, the processor area to pre-store a first key-share therein;

a module receiving area to receive a subscriber identity module (SIM), the SIM having a second key-share pre-stored therein; and

an RF interface to receive a third key-share and encrypted content over a wireless communication link in response to a request for content and verification of a user's credit,

wherein the security processor is to combine the first, second and third key-shares to decrypt the encrypted content and monitor playing of the decrypted content by the communications processor against measurement parameters, and

wherein the security processor is to further authenticate the measurement parameters using an authentication code to help prevent tampering with the measurement parameters, the measurement parameters being secured by the authentication code and provided by a security server over the wireless communication link along with the encrypted content.[[,,]] ~~and~~

~~wherein the first key-share is pre-stored in the processor area and the second key-share is pre-stored in the SIM prior to the device generating the request for the content and prior to a security server sending the content and the third key-share to the wireless communication device.~~

22. (Currently Amended) A wireless communication device as claimed in claim 21 wherein the security processor purges at least one of the key-shares when usage of the content exceeds a service limit indicated by the measurement parameters, or when the authentication code fails to authenticate, and

wherein the first key-share is pre-stored in the processor area and the second-key-share is pre-stored in the SIM prior to the wireless device generating the request for the content and prior to a security server sending the content and the third-key-share to the wireless communication device.

23. (Previously Presented) A wireless communication device as claimed in claim 21 wherein the processor area receives the third key-share from a finance server when a user is approved for use of the content in accordance with the measurement parameters.

24. (New) A wireless communication device as claimed in claim 21 wherein communications between the security processor and the communication processor take place within the processor area to inhibit unauthorized interception of the decrypted content and interception of the first key-share stored in the processor area.

25. (New) A wireless communication device comprising:

a processor area of an integrated circuit having a communications processor and security processor, the processor area to pre-store a first key-share therein;

a module receiving area to receive a subscriber identity module (SIM), the SIM having a second key-share pre-stored therein; and

an RF interface to receive a third key-share and encrypted content over a wireless communication link in response to a request for content and verification of a user's credit,

wherein the security processor is to combine the first, second and third key-shares to decrypt the encrypted content and monitor playing of the decrypted content by the communications processor against measurement parameters, and

wherein communications between the security processor and the communication processor take place within the processor area to inhibit unauthorized interception of the decrypted content and interception of the first key-share stored in the processor area.

26. (New) The wireless communication device of claim 25 wherein the security processor and the communication processor are fabricated as an application specific integrated circuit (ASIC) that includes the processor area.

27. (New) The wireless communication device of claim 25 wherein the security processor is to further authenticate the measurement parameters using an authentication code to help prevent tampering with the measurement parameters, the measurement parameters being secured

by the authentication code and provided by a security server over the wireless communication link along with the encrypted content, and

wherein the first key-share is pre-stored in the processor area and the second-key-share is pre-stored in the SIM prior to the device generating the request for the content and prior to a security server sending the content and the third-key-share to the wireless communication device.